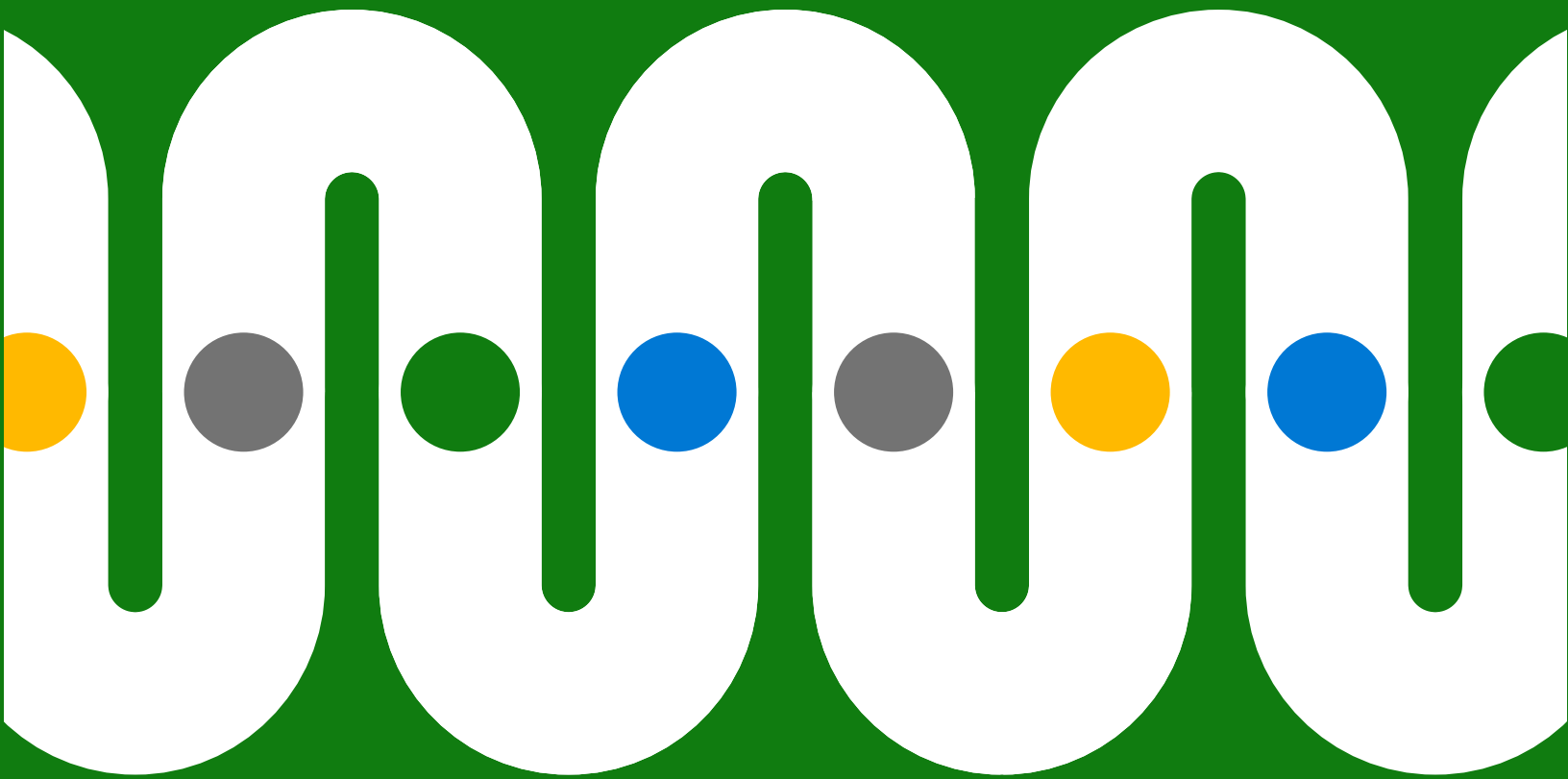
Microsoft Security

3 Steps for Protecting Your Data End to End



Contents

A survey of compliance decision-makers showed that 95% were concerned about data-protection challenges.[2]

Introduction

Organizations have seen a massive increase in their digital footprint with hybrid work, extending well beyond the traditional office.

That's led to more data fragmentation and exfiltration—all complicated by rapid growth across a multitude of applications, devices, and locations. Many workers have also switched roles in search of greater fulfillment or flexibility, and that's added to these challenges, creating new blind spots across ever-growing data estates.[1]

All these factors have CIOs and CISOs rethinking their approach to information protection. In a tracking survey of over 500 US compliance decision-makers, nearly all (95 percent) were concerned about data-protection challenges.[2]

[1] "How Microsoft can help reduce insider risk during the Great Reshuffle, Alym Rayani", Microsoft Security. February 28, 2022.

[2] "September 2021 survey of 512 US compliance decision-makers commissioned by Microsoft from Vital Findings".

IT and security teams are looking for better ways to manage the entire data lifecycle, across multicloud, hybrid cloud, and on-premises environments. This end-to-end approach involves three key steps:

Step 1: Identify data

Determine where your data lives, what kind of data it is, and how it's being used or shared

Step 2: Classify data

Classify and label data so that you know the right policies and risk mitigation to apply

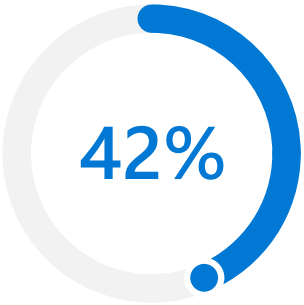
Step 3: Prevent data loss

Strike a balance between risk-reduction and flexibility for your people with intelligent detection and control

The goal of this approach? To close gaps and minimize risk without sacrificing productivity.

Step 1

Identify data



When asked how much of their data is "dark," 42% of organizations said at least half.[3]

This "hidden" data can take many forms—from email attachments and customer call records to machine logs and video footage.

If you can't identify your data—where it lives, what type it is, and how it's being used or shared—it's impossible to apply the right policies or protection.

Modern organizations continuously generate vast amounts of data. It's not just documents, emails, and messages, but everything from security footage to geolocation data, all compounded by proliferation across apps, devices, and storage, on premises and in the cloud.

Identifying all this data can be difficult, and 42 percent of organizations say that at least half of their data is "dark."[3] That is, information collected but unknown or unused for business purposes. Sometimes data becomes dark when the worker who created it switches projects or roles; often there are simply no systems in place to identify data at the point of creation or modification.

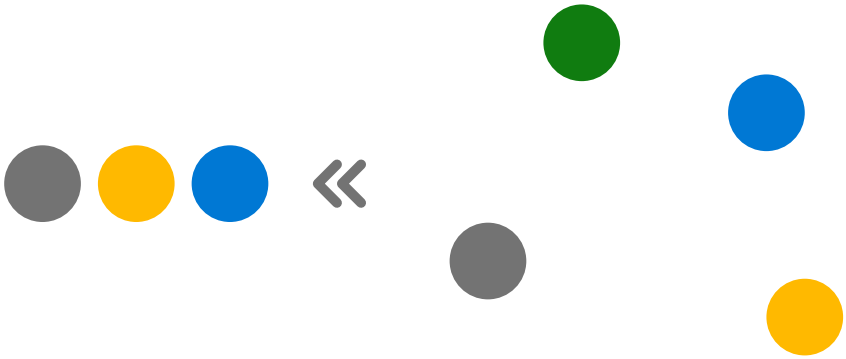
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. July 2022.

Want to build an end-to-end discovery workflow on one platform?

Learn about data discovery in Microsoft Purview at **Microsoft.com**.

This challenge will only grow. The amount of new data that's created, captured, replicated, and consumed is expected to more than double by 2026, with enterprise data growing more than twice as fast as consumer data.[4]

Artificial intelligence (AI) and machine learning (ML) can help, by recognizing sensitive data—such as email addresses, health data, credit card numbers, or intellectual property— and classifying it automatically. These identification processes can span your entire data estate, finding, labeling, and protecting data anywhere it lives, across any clouds.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. May 2022.

Step 2

Classify data

Classifications and policies both need to follow data as it travels.

For example, if an employee copies credit card numbers from a Microsoft Word document into Excel, the classification and policies should automatically apply to both documents.

Proper data classification helps you determine the right policies and risk mitigation for ensuring different types of data aren't accidentally or intentionally misused or accessed without authorization. Encryption and watermarking can protect data even further—whether it's at rest, in transit, or in use.

But classification and policies need to follow data as it travels around the organization. Labeling and protection policies can't be confined to discrete documents, they need to span your entire digital estate—from on-premises to cloud-based repositories, from software-as-a-service (SaaS) to OS-native apps.

Traditional classification approaches involve considerable manual work, which runs the risk of errors or inadvertently overlooking critical data. Built-in and trainable classifiers can help automate this process, and an integrated solution allows administrators to manage policies centrally, across all systems.

Want to better manage and protect sensitive data across your environment?

Learn about data classification and protection in Microsoft Purview at **Microsoft.com**.

Step 3

Prevent data loss

DLP policy can prevent out-of-compliance actions.

For example, if an employee tries to download a spreadsheet with credit card numbers onto a flash drive or upload it to cloud storage, DLP policy could identify the activity as out of compliance and prevent it.

Want intelligent detection and control of sensitive information?

Learn about data loss prevention in Microsoft Purview at **Microsoft.com**.

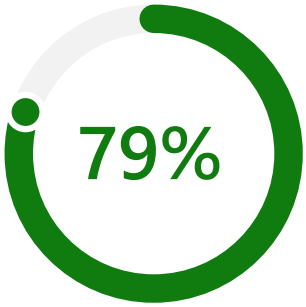
Once you've identified and classified your data, data loss prevention (DLP) solutions can enforce end-to-end protection policies that mitigate threats like dark data and data exfiltration, so current and former employees do not—intentionally or inadvertently—share, expose, or transfer sensitive data without authorization.

Intelligent DLP solutions use context to strike a balance between providing flexibility and blocking high-risk actions. For example, individuals might be able to continue with an action after being reminded about potential risks and applicable policies. This can help protect sensitive data while also training users to better understand risk.

DLP solutions help protect intellectual property and other critical business data, while also improving compliance with regulations such as the General Data Protection Regulation (GDPR), Health Information Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA).

A comprehensive approach to DLP enforces policies across your organization consistently, protecting the "weakest link" points in the data lifecycle.

Don't bolt data protection on. Build it in.



A survey of compliance decision-makers showed that 79% had purchased multiple compliance and data-protection products.

A majority had purchased three or more.[5]

Many organizations have tried a "bolt-on" approach to information protection, using multiple solutions to manage discrete parts of the data lifecycle. But this forces your security, data governance, compliance, and legal teams to stitch together a patchwork that's often ineffective and strains resources.

A "built-in" approach can close the gaps, bringing together data identification, data classification, and DLP. With an integrated solution, it's easier to centrally manage and enforce policies. It also reduces training time for users, who receive policy notifications in a familiar way, natively within applications.

[5] "February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research."

A built-in, integrated solution: Microsoft Purview

Microsoft Purview helps you meet the challenges of today's decentralized, data-rich workplace, with a comprehensive set of solutions that help you govern, protect, and manage your entire data estate.

Go beyond governance.

Learn more about protecting your data with Microsoft Purview >

Interested in a specific area of data protection? Get more detailed information on how Microsoft Purview can help you with:

Data discovery >

Data classification and protection >

Data loss prevention >

Microsoft Security